JOURNAL OF NUMBER THEORY 32, 65–77 (1989)

Iwasawa Invariants of CM Fields

JAMES S. KRAFT

Department of Mathematics, Saint Mary's College of California, Moraga, California 94575

Communicated by H. Zassenhaus

Received August 14, 1987

Let K be a CM field with K^+ its maximal real subfield. Let λ, λ^+ be the Iwasawa λ-invariants for the cyclotomic $\mathbb{Z}_p$-extension of K, K^+, respectively. We set $\lambda^- = \lambda - \lambda^+$. We show that under certain conditions, $\lambda^+ \leqslant \lambda^- - 1$. We use this inequality to give criteria which imply that $\lambda^+ = 0$. © 1989 Academic Press, Inc.

1. INTRODUCTION

Let K be a number field. We say that K_∞/K is a $\mathbb{Z}_p$-extension if K_∞/K is a Galois extension whose Galois group is isomorphic to $\mathbb{Z}_p$, the additive group of p-adic integers. Then for every non-negative integer n, there is a unique number field K_n with $K \subset K_n \subset K_\infty$ and $\mathrm{Gal}(K_n/K)$ cyclic of order p^n. If p^{e_n} is the highest power of p dividing the class number of K_n, Iwasawa has proved that there are integers μ, λ, and ν, independent of n such that $e_n = \mu p^n + \lambda n + \nu$ for all n sufficiently large. Then μ, λ, and ν are called the Iwasawa invariants associated to the $\mathbb{Z}_p$-extension K_∞/K for the prime p. It is natural to ask when it is possible to determine the values of these invariants. In this paper, we will analyze this question.

We now fix a totally real number field k, an odd prime p, and a number field K which is an abelian extension of k containing ζ_p. Our study of the Iwasawa invariants is based on the following. Let X be the Galois group of the maximal abelian unramified p-extension of K_∞. Then X is a module over $\Lambda = \mathbb{Z}_p[[T]]$ and associated to X is a characteristic power series $f(T)$. We may write $f(T) = p^\mu g(T) U(T)$ with $U(T)$ a unit in Λ and $\deg(g(T)) = \lambda$. Thus, in order to compute μ and λ, it is sufficient to know $f(T)$.

If K^+ is the maximal real subfield of K, we let μ^+ and λ^+ be the Iwasawa invariants of K^+. We assume that $\Delta = G(K/k)$ has order prime to p. If $\hat{\Delta}$ is the group of p-adic characters of Δ, and $\varphi \in \hat{\Delta}$, then there is a power series $f_\varphi(T)$ which is the characteristic power series associated to

0022-314X/89 $3.00

$X(\varphi)$. Let $f^-(T)=\prod_{\varphi\in\hat{\Delta},\varphi\,\text{odd}} f_\varphi(T)$ and let $f^+(T)=\prod_{\varphi\in\hat{\Delta},\varphi\,\text{even}} f_\varphi(T)$. Then, as above, $f_\varphi(T)=p^{\mu_\varphi}g_\varphi(T)U_\varphi(T)$.

We note that $\mu^+=\sum_{\varphi\,\text{even}}\mu_\varphi$ and $\lambda^+=\sum_{\varphi\,\text{even}}\lambda_\varphi$. If $\mu^-=\mu-\mu^+$ and $\lambda^-=\lambda-\lambda^+$, we see that $\mu^-=\sum_{\varphi\,\text{odd}}\mu_\varphi$ and $\lambda^-=\sum_{\varphi\,\text{odd}}\lambda_\varphi$.

Let $\omega, \chi\in\hat{\Delta}$ be the Teichmüller character and an even character, respectively, and let $\psi=\chi\omega^{-1}$. In Theorems 1 and 2 of this paper, we show that certain constraints on the fixed field of the kernel of ψ and on the fixed field of the kernel of χ will allow us to conclude that up to multiplication by a unit, $f_\psi(T)$ is linear and prime to p. This tells us that $\mu_\psi=0$ and that $\lambda_\psi=1$.

A conjecture of Greenberg asserts that $\lambda^+=0$. In Theorem 3, we give conditions which imply that $\lambda^+\leqslant\lambda^- -1$. We then give criteria which imply that $\lambda^-=1$. This, coupled with our previous inequality, enables us to state sufficient conditions for Greenberg's conjecture to be true.

In Section 10 we give a brief discussion of p-adic L-functions, and show how our results give information concerning their zeros.

We conclude by specializing our results to quadratic fields and giving several examples.

2. Basic Iwasawa Theory

Let k be a number field and let k_∞/k be a $\mathbb{Z}_p$-extension with k_n the unique subfield of k_∞ of degree p^n over k. Let L_∞ be the maximal abelian unramified p-extension of k_∞ and let $X=\mathrm{Gal}(L_\infty/k_\infty)$. X may be viewed as a module over $\mathbb{Z}_p[[\Gamma]]$ where $\Gamma=\mathrm{Gal}(k_\infty/k)$. If γ_0 is a fixed topological generator of Γ, then X may also be thought of as a module over the formal power series ring $\Lambda=\mathbb{Z}_p[[T]]$, where T acts as γ_0-1.

It is well known that X is a finitely generated torsion Λ-module. As such there is a pseudo-isomorphism (recall that a pseudo-isomorphism is a homomorphism with finite kernel and cokernel) $\varphi\colon X\to\Lambda/(f(T))$. Iwasawa theory tells us that $f(T)=p^\mu g(T)U(T)$ where μ is a non-negative integer, $g(T)=T^\lambda+a_{\lambda-1}T^{\lambda-1}+\cdots+a_0$ with $a_i\equiv 0 \pmod p$, $0\leqslant i\leqslant\lambda-1$, and $U(T)\in\Lambda^\times$. The polynomial $g(T)$ is called distinguished. Note that μ (resp. λ) is the Iwasawa μ-invariant (resp. Iwasawa λ-invariant) for the $\mathbb{Z}_p$-extension k_∞/k.

3. Some Remarks on X^-

We begin by assuming that for each n, k_n is a CM-field. Let k_n^+ be its maximal real subfield and let A, A_n^+ be the p-Sylow subgroup of the class group of k_n, k_n^+, respectively. We assume from now on that p is an odd prime. Let A_n^- be the kernel of the norm map from k_n to k_n^+. Then $A_n \simeq A_n^+ \oplus A_n^-$.

Let X_n, X_n^+ denote the Galois group of the maximal abelian unramified p-extension of k_n, k_n^+, respectively. Then $X_n \simeq A_n$, $X_n \simeq X_n^+ \oplus X_n^-$, and noting that $X \simeq \varprojlim X_n$, we see that $X \simeq X^+ \oplus X^-$.

LEMMA 1. *Let K_∞/K be a $\mathbb{Z}_p$-extension with K and K_∞ CM fields. Suppose that exactly one prime ramifies in K_∞/K and assume that it totally ramifies. If A_0^- is cyclic, then $X^- \simeq \Lambda/(p^\mu g(T))$ where $g(T)$ is a distinguished polynomial.*

Proof. Clearly we may assume that X^- is non-zero. From the fact that one prime ramifies and totally ramifies, we see that $A_0^- \simeq X^-/TX^-$. Thus, X^-/TX^- is cyclic as a $\mathbb{Z}$-module, and from Nakayama's lemma we have that X^- is cyclic as a Λ-module.

So, $\Lambda/I \simeq X^-$ for I an ideal in Λ. If I were not principal, there would be a non-zero f and g in I with $h = \gcd(f, g) \notin I$. If $f = f_1 h$ and $g = g_1 h$ we then see that $\Lambda/(f_1, g_1)$ is finite, and hence so is $\langle h, I\rangle/I$. Since $X^- \simeq \Lambda/I$ we would then have X^- containing a finite Λ-module which is impossible. Hence, $I = (f(T))$ and via the p-adic Weierstrass preparation theorem, $f(T) = p^\mu g(T) U(T)$ with $g(T)$ a distinguished polynomial and $U(T) \in \Lambda^\times$. ∎

Remark. Using the notation of the next section, if φ is an odd character, the same proof works if X^- is replaced by $X(\varphi)$, K is replaced by K^φ, and A_0^- is replaced by $A_0(\varphi)$.

This lemma will be important later on since it will allow us to retrieve information about every level of a $\mathbb{Z}_p$-tower from knowledge of the base field.

4. CHARACTERS AND IDEMPOTENTS

We now assume that k is a totally real number field, K is an abelian extension of k which contains a primitive pth root of unity ζ_p, and that p does not divide $|K : k|$. Let $\Delta = G(K/k)$ and let $\hat{\Delta}$ denote the group of p-adic characters of Δ. If $J \in \Delta$ is complex conjugation and M is any Δ-module, we may write $M = M^+ \oplus M^-$ where $M^+ = [(1+J)/2]M$ and $M^- = [(1-J)/2]M$.

If $\varphi \in \hat{\Delta}$, let ε_φ be the 1-dimensional orthogonal idempotent corresponding to φ. For simplicity of the exposition, we assume that the values of φ are in $\mathbb{Z}_p$. If this is not the case, everything still works with $\mathbb{Z}_p$ replaced by $\mathbb{Z}_p$ with the values of φ adjoined and Λ replaced by Λ with the values of φ adjoined. If $\mathbb{Z}_p[\varphi]$ denotes the former, then note that $\mathbb{Z}_p[\varphi]/p\mathbb{Z}_p[\varphi]=p^n$ where $n=[\mathbb{Q}_p[\varphi]:\mathbb{Q}_p]$, so that all the index calculations must be modified. Let $M(\varphi)=\varepsilon_\varphi(M)$.

If $\varphi(J)=1$ we say that φ is an even character, and if $\varphi(J)=-1$ we say that φ is an odd character. Then $M^+=\bigoplus_{\varphi\in\hat{\Delta},\varphi \text{even}} M(\varphi)$ and $M^-=\bigoplus_{\varphi\in\hat{\Delta},\varphi \text{odd}} M(\varphi)$. Finally, we denote by K^φ the fixed field of the kernel of φ, so that $k\subseteq K^\varphi\subseteq K$.

Let K_∞ be the cyclotomic $\mathbb{Z}_p$-extension of K. Since $\zeta_p\in K$, the group W of all p-power roots of unity is contained in K_∞. If $\mathscr{G}_\infty=\mathrm{Gal}(K_\infty/k)$, we have $\mathscr{G}_\infty\simeq\Delta\times\Gamma$.

Let $\kappa\colon\mathscr{G}_\infty\to\mathbb{Z}_p^\times$ be defined by $g(\zeta)=\zeta^{\kappa(g)}$ for all $g\in\mathscr{G}_\infty$ and $\zeta\in W$. We denote by ω the restriction of κ to Δ. ω is the Teichmüller character.

Let $\chi\in\hat{\Delta}$ be any non-trivial even character, and let A_0 be the p-Sylow subgroup of the class group of K. Then $A_0(\omega\chi^{-1})$ occurs as a direct summand of the p-Sylow subgroup of the class group of $K^{\omega\chi^{-1}}$. In fact, we have the following.

Lemma 2. *Let $\varphi\in\hat{\Delta}$ be any character, and let A_0 be the p-Sylow subgroup of the class group of K. If $A_0(K^\varphi)$ denotes the p-Sylow subgroup of the class group of K^φ, then $\varepsilon_\varphi(A_0)\simeq\varepsilon_\varphi(A_0(K^\varphi))$.*

Proof. Let N_φ be the norm map from K to K^φ. Then, since p does not divide the order of Δ, we have a short exact sequence

$$0\to\ker(N_\varphi)\to A_0\to A_0(K^\varphi)\to 0.$$

Since this sequence clearly splits, $A_0\simeq A_0(K^\varphi)\oplus\ker(N_\varphi)$.

An easy calculation shows that $\varepsilon_\varphi N_\varphi=|\ker(\varphi)|\varepsilon_\varphi$. Since p and $|\Delta|$ are relatively prime, $|\ker(\varphi)|\,\varepsilon_\varphi M=\varepsilon_\varphi M$ for any $\mathbb{Z}_p[\Delta]$-module M. Thus, $\varepsilon_\varphi(M)=\varepsilon_\varphi N_\varphi(M)$. So, $\varepsilon_\varphi[\ker(N_\varphi)]=0$, and Lemma 2 is proven. ∎

Since $\omega\chi^{-1}$ is an odd character, if we assume that $A_0(\omega\chi^{-1})$ is cyclic and that one prime ramifies and that it totally ramifies in $K_\infty^{\omega\chi^{-1}}/K^{\omega\chi^{-1}}$, the remark after Lemma 1 says that $X(\omega\chi^{-1})\simeq\Lambda/(p^{\mu_{\omega\chi^{-1}}}g_{\omega\chi^{-1}}(T))$, where $\mu_{\omega\chi^{-1}}$ is a non-negative integer and $g_{\omega\chi^{-1}}(T)$ is a distinguished polynomial.

5. Kummer Theory

Keeping the notation from the previous section, $W\subset K_\infty$ where W is the group of all p-power roots of unity. Let M_∞ be the maximal abelian p-extension of K_∞ which is unramified outside p, and let $X_\infty=\mathrm{Gal}(M_\infty/K_\infty)$.

Since $W\subset K_\infty$, M_∞/K_∞ is a Kummer extension. Thus, there is a subgroup $V \subseteq K_\infty^\times \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p)$ and a non-degenerate bilinear pairing $(\ ,\ ): X_\infty \times V \to W$ with the property that $(gx, gv) = (x, v)^g$ for all $x \in X_\infty$, $v \in V$, and $g \in \mathscr{G}_\infty$. Thus, $X_\infty \simeq \mathrm{Hom}(V, W)$ and $X_\infty(\chi) \simeq \mathrm{Hom}(V(\omega\chi^{-1}), W)$. Since $\omega\chi^{-1}$ is odd, $V(\omega\chi^{-1}) \simeq A_\infty(\omega\chi^{-1})$, and so $X_\infty(\chi) \simeq \mathrm{Hom}(A_\infty(\omega\chi^{-1}), W)$.

6. Twisting

We now introduce the Pontryagin dual of $A_\infty(\omega\chi^{-1})$ which is defined to be $\mathrm{Hom}(A_\infty(\omega\chi^{-1}), \mathbb{Q}_p/\mathbb{Z}_p) = A_\infty(\omega\chi^{-1})^\wedge$. Let $\mathscr{G}_\infty$ act on $A_\infty(\omega\chi^{-1})^\wedge$ via $(gf)(a) = f(ga)$ where $g \in \mathscr{G}_\infty$, $f \in A_\infty(\omega\chi^{-1})^\wedge$, and $a \in A_\infty(\omega\chi^{-1})$. We claim that $A_\infty(\omega\chi^{-1})^\wedge \simeq X(\omega\chi^{-1})$. In order to show this, we need to define the adjoint.

Let M be any Λ-module. Consider the map $\psi: M \to \prod_p M_p$ where the product is taken over all primes of height one in Λ and M_p denotes the localization of M at p. The adjoint of M, $\alpha(M)$, is defined to be the cokernel of ψ. The following facts are well known (for their proofs, see [Fe]).

First, if $P_n(T) = (1+T)^{p^n} - 1$, then $\alpha(M) \simeq \mathrm{Hom}[\varinjlim M/(P_n(T))M, \mathbb{Q}_p/\mathbb{Z}_p]$. Second, if $M \simeq \Lambda/(g(T))$ with $g(T) \in \Lambda$, then $\alpha(M) \simeq M$.

We now consider $A_\infty(\omega\chi^{-1})^\wedge$. Since one prime ramifies and totally ramifies in $K_\infty^{\omega\chi^{-1}}/K^{\omega\chi^{-1}}$, it is well known that $A_n(\omega\chi^{-1}) \simeq X(\omega\chi^{-1})/(P_n(T))X(\omega\chi^{-1})$ (see [Wa 1, p. 284]). Thus, $A_\infty(\omega\chi^{-1})^\wedge = \mathrm{Hom}[A_\infty(\omega\chi^{-1}), \mathbb{Q}_p/\mathbb{Z}_p] = \mathrm{Hom}[\varinjlim A_n(\omega\chi^{-1}), \mathbb{Q}_p/\mathbb{Z}_p] = \mathrm{Hom}[\varinjlim X(\omega\chi^{-1})/(P_n(T))X(\omega\chi^{-1}), \mathbb{Q}_p/\mathbb{Z}_p] \simeq \alpha(X(\omega\chi^{-1}))$. But the remark following Lemma 1 says that $X(\omega\chi^{-1}) \simeq \Lambda/(f(T))$ for some $f(T)$. Thus, $\alpha(X(\omega\chi^{-1})) \simeq X(\omega\chi^{-1})$. We then have $A_\infty(\omega\chi^{-1})^\wedge \simeq X(\omega\chi^{-1})$. Since $X(\omega\chi^{-1}) \simeq \mathrm{Hom}[A_\infty(\omega\chi^{-1}), \mathbb{Q}_p/\mathbb{Z}_p]$, we have a non-degenerate bilinear pairing $X(\omega\chi^{-1}) \times A_\infty(\omega\chi^{-1}) \to \mathbb{Q}_p/\mathbb{Z}_p$. We refer to this as the $\mathbb{Q}_p/\mathbb{Z}_p$-pairing.

At the end of the previous section we had another non-degenerate bilinear pairing $X_\infty(\chi) \times A_\infty(\omega\chi^{-1}) \to W$. We refer to this as the W-pairing.

$\mathrm{Hom}(A_\infty(\omega\chi^{-1}), W)$ has the structure of a $\mathscr{G}_\infty$-module via $(gf)(a) = g(f(g^{-1}a))$. We then see that the W-pairing satisfies $(gx, a) = (x, \kappa(g)\, g^{-1}a)$ where $g \in \mathscr{G}_\infty$, $x \in X_\infty(\omega\chi^{-1})$, and $a \in A_\infty(\omega\chi^{-1})$, while the $\mathbb{Q}_p/\mathbb{Z}_p$-pairing has the property that $(gx, a) = (x, ga)$ where $g \in \mathscr{G}_\infty$, $x \in X(\omega\chi^{-1})$, and $a \in A(\omega\chi^{-1})$. We now play off these two different actions and show that $X_\infty(\chi) \simeq \Lambda/(f(\kappa_0(1+T)^{-1} - 1))$. Similar situations have been considered by Greenberg [Gr 3].

Let $h(T) \in \Lambda$ have the property that $h(T)X_\infty(\chi) = 0$. Recalling that $1+T$ corresponds to γ_0, we see that the non-degeneracy of the W-pairing tells us that $h(\kappa_0\gamma_0^{-1} - 1)A_\infty(\omega\chi^{-1}) = 0$. The $\mathbb{Q}_p/\mathbb{Z}_p$-pairing now says that the $h(\kappa_0\gamma_0^{-1} - 1)X(\omega\chi^{-1}) = 0$. But $X(\omega\chi^{-1}) \simeq \Lambda/(f(t))$. Thus $f(T)$ divides $h(\kappa_0(1+T)^{-1} - 1)$. A change of variables shows that $f(\kappa_0(1+T)^{-1} - 1)$

divides $h(T)$. The non-degeneracy of the $\mathbb{Q}_p/\mathbb{Z}_p$-pairing shows that this argument is reversible, so that the annihilator of $X_\infty(\chi)$ is $f(\kappa_0(1+T)^{-1}-1)$. Thus, we will be done if we can show that $X_\infty(\chi)$ is cyclic as a Λ-module. So, we will now prove this.

Let K' be the maximal abelian unramified outside p extension of K which is of exponent p. Then $H = G(K'/K) \simeq A/A^p$, where A is the p-Sylow subgroup of the class group of K'. Moreover, $H \simeq A/A^p$ as $\mathbb{Z}_p[\Delta]$-modules.

By Kummer theory, there is a subgroup $B \subseteq K^\times/(K^\times)^p$ with $K' = K(\sqrt[p]{B})$ and a non-degenerate bilinear pairing $H \times B \to W_p = p$th roots of unity. Let $A_p = \{x \in A \mid x^p = 1\}$. Then there is a surjective map $\varphi\colon B \to A_p$ whose kernel is contained in E/E^p where E is the group of units of K. Since $\omega\chi^{-1}$ is odd, and $\omega\chi^{-1} \neq \omega$, $B(\omega\chi^{-1}) \simeq A_p(\omega\chi^{-1})$. By assumption, $|A_p(\omega\chi^{-1})| = p$ so that $|B(\omega\chi^{-1})| = p$ as well.

The pairing gives rise to a pairing between $B(\omega\chi^{-1})$ and $H(\chi)$ which is easily seen to be $X_\infty(\chi)/(p, T)$. Thus $X_\infty(\chi)(p, T)$ is of order p, hence cyclic. Nakayama's lemma now says that $X_\infty(\chi)$ is cyclic as a Λ-module as asserted.

We summarize the results from this section and the previous section as a theorem.

THEOREM 1. *Let k be a totally real number field and let K be a finite abelian extension of k which contains ζ_p. We assume that p does not divide $|\Delta| = |G(L/K)|$. Let $\chi \in \hat{\Delta}$ be a non-trivial even character. Let A_0 be the p-Sylow subgroup of the class group of K, and assume that $A_0(\omega\chi^{-1})$ is cyclic. Let $K_\infty^{\omega\chi^{-1}}/K^{\omega\chi^{-1}}$ be the cyclotomic $\mathbb{Z}_p$-extension, and assume that one prime ramifies in $K_\infty^{\omega\chi^{-1}}/K^{\omega\chi^{-1}}$ and that it totally ramifies. Then $X_\infty(\chi) \simeq \Lambda/f(\kappa_0(1+T)^{-1}-1)$ where $X(\omega\chi^{-1}) \simeq \Lambda(f(T))$.*

7. A COMPUTATION OF $f(T)$

Theorem 1 tells us that there is a relationship between unramified outside p-extensions on the "plus" side and unramified extensions on the "minus" side. We will now exploit this relationship and obtain information about $f(T)$.

From now on we assume that χ is a non-trivial even character which generates the group of characters of $G(K^\chi/k)$. If A is the p-Sylow subgroup of the class group of A, let $h(\chi) = |A(\chi)|$ and let $\Delta(\chi)$ be the discriminant of K^χ.

Let S be the set of primes in K^χ which lie over p, let E_1 be the group of units of K^χ which are congruent to $1 \bmod \mathfrak{p}$ for each $\mathfrak{p} \in S$, and let $\varphi\colon K^\chi \to \prod_{\mathfrak{p} \in S} K_\mathfrak{p}^\chi$ be the canonical embedding where $K_\mathfrak{p}^\chi$ is the completion of K^χ at $\mathfrak{p}$. Let D be the $\mathbb{Z}_p$-module generated by $\varphi(E_1)$ and $\varphi(\varepsilon_d)$ where

$\varepsilon_d = 1+p$. We denote by φ_p the canonical embedding of K in K_p and by log the p-adic logarithm. Then if $\varepsilon_1, \ldots, \varepsilon_{d-1}$ is a $\mathbb{Z}$-basis for E_1, we can write $\log \varphi_p(\varepsilon_j) = \sum_{k=1}^{dp} b_{jk}^{(p)} \alpha_k$ where $d_p = [K_p^\chi : \mathbb{Q}_p]$, the $b_{jk}^{(p)}$ are in $\mathbb{Q}_p$, and the a_k form a $\mathbb{Z}_p$-basis for $\mathcal{O}_p$. So, for each $p \in S$ we can construct a matrix whose entries are the b_{jk}^p. Let B be the direct sum of all of these matrices. Then $|\det(B)| = (R_p/\sqrt{\Delta(\chi)})\, dpu$ where $d = [K^\chi : \mathbb{Q}]$, R_p is the p-adic regulator of K^χ, and u is a p-adic unit. If $\Omega = \prod_{p \in S} \mathcal{O}_p$, then $|\det(B)| = |\Omega : \log D|$ as well. Thus $|\Omega : \log D| = (R_p/\sqrt{\Delta(x)})\, dpu$. So we have the following definition.

Definition. $(R_p/\sqrt{\Delta(\chi)})(\chi) = |\Omega(\chi) : \log D(\chi)|$.

Let S_k be the set of primes in k which lie over p, and let $F(\chi) = |h(\chi)((R_p/\sqrt{\Delta(\chi)})(\chi)) \prod_{p_k \in S_k} [1 - \chi(p_k)/N_{p_k}]\, |_p^{-1}$ where $|\ \ |_p$ is the p-adic absolute value normalized so that $|p|_p = 1/p$.

The following proposition is essentially due to Coates. ([Co]). It follows from his result by taking the χ-eigenspace of all appropriate terms.

Proposition 1. *Let M_∞^χ be the maximal abelian p-extension of K^χ which is unramified outside p. Then $G(M_\infty^\chi/K_\infty^\chi)$ is finite if and only if $R_p(K^\chi)$ is non-zero, i.e., if and only if Leopoldt's conjecture is true for K^χ. If $R_p(K^\chi) \neq 0$, then $|G(M_\infty^\chi/K_\infty^\chi)(\chi)| = F(\chi)$.*

Recall that Theorem 1 says that under certain conditions, $X_\infty(\chi) \simeq \Lambda/(f(\kappa_0(1+T)^{-1}-1))$. We now make a choice for γ_0 and hence for κ_0 by setting $e = \max\{n \mid K^\chi(\zeta_p) \supseteq \mathbb{Q}(\zeta_{p^n})\}$. Certainly $e \geqslant 1$, and we may take $\kappa_0 = 1 + p^e$.

Theorem 2. *We retain all the hypotheses of Theorem 1. Assume that $A_0(\omega\chi^{-1})$ is not only cyclic but has order exactly p. If $F(\chi) = p^n$ with $n \geqslant e+1$, then $f(T) = (T-a)U(T)$ with $U(T) \in \Lambda^\times$, i.e., $\mu_{\omega\chi^{-1}} = 0$ and $\lambda_{\omega\chi^{-1}} = 1$. Also, $e = 1$ and $a \equiv p (\mathrm{mod}\, p^n)$.*

Proof. It is not hard to see that $X_\infty(\chi)/T \cdot X_\infty(\chi)$ is the largest quotient on which Γ acts trivially. Then, since M_∞^χ is the maximal abelian p-extension of K^χ unramified outside p, $G(M_\infty^\chi/K_\infty^\chi)(\chi) \simeq X_\infty(\chi)/T \cdot X_\infty(\chi)$. We first assume that $(R_p/\sqrt{\Delta(\chi)})(\chi) \neq 0$. Then, from Lemma 2, $|G(M_\infty^\chi/K_\infty^\chi)| = F(\chi) = p^n$. Thus, $|X_\infty(\chi)/T \cdot X_\infty(\chi)| = p^n$. Since $X_\infty(\chi) \simeq \Lambda/(f(\kappa_0(1+T)^{-1}-1))$, we see that $|\mathbb{Z}_p/f(p^e)\mathbb{Z}_p| = p^n$.

Recall that $f(T) = p^\mu g(T) U(T)$ with μ a non-negative integer, $U(T) \in \Lambda^\times$, and $g(T) = a_0 + a_1 T + \cdots + a_{k-1} T^{k-1} + T^k$ with $a_i \equiv 0 (\mathrm{mod}\, p)$ for $0 \leqslant i \leqslant k-1$. Thus, we must show that $\mu = 0$ and $k = 1$.

Since $A_n(\omega\chi^{-1}) \simeq \Lambda/(P_n(T), f(T))$ where $P_n(T) = (1+T)^{p^n} - 1$, we see that $A_0(\omega\chi^{-1}) \simeq \Lambda/(T, f(T))$. Since $|A_0(\omega\chi^{-1})| = p$, we have that $f(0) \equiv 0 (\mathrm{mod}\, p)$ but $f(0) \not\equiv 0 (\mathrm{mod}\, p^2)$. These two congruences, together with the fact that $n \geqslant e+1 \geqslant 2$, immediately tell us that $\mu = 0$ and $k = 1$. In fact, even more can be said. Since $f(p^e) \equiv 0 (\mathrm{mod}\, p^n)$, $e = 1$ and $f(T) = (T-u) U(T)$ with $a \equiv p (\mathrm{mod}\; p^n)$. This will be of interest when we discuss p-adic L-functions.

We now examine the possibility that $(R_p/\sqrt{\Delta(\chi)})(\chi) = 0$. In this case, Proposition 1 tells us that $|G(M_\infty^\chi / K_\infty^\chi)|$ has infinite order. Thus, $|X_\infty(\chi)/TX_\infty(\chi)| > p^n$ for every positive integer n, so that $|\mathbb{Z}_p / f(p^e)\mathbb{Z}_p| > p^n$.

The same argument used when $(R_p/\sqrt{\Delta(\chi)})(\chi) \neq 0$ then gives us that $f(T) = (T-a) U(T)$ with $U(T) \in \Lambda^\times$ and $a = p^e$. ∎

It is possible to obtain information about $f(T)$ if we allow $A_0(\omega\chi^{-1})$ to be cyclic p-group whose order is greater than p. For example, assume that $|A_0(\omega\chi^{-1})| = p^2$. Then if $F(\chi) = p^n$ with $n \geqslant e+2$, the same techniques show that $\lambda \geqslant 2$.

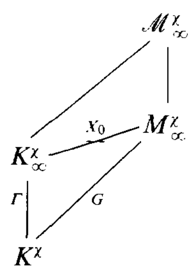
The Iwasawa invariant μ associated to the cyclotomic $\mathbb{Z}_p$-extension of an abelian number field is zero. Theorem 2 can be used to obtain information on the vanishing of μ for the cyclotomic $\mathbb{Z}_p$-extension of any number field. For example, k could be an arbitrary totally real number field so that k may not even be a Galois extension of $\mathbb{Q}$.

8. Some Results on λ^+

Theorem 2 is a theorem about growth on the "minus" side of the $\mathbb{Z}_p$-extension. We now obtain information concerning the "plus" side.

Theorem 3. *Maintaining the hypotheses of Theorem* 1, *we assume that one prime ramifies and that it totally ramifies in* K_∞^χ / K^χ. *If* $F(\chi)/|A_0(\chi)| = p^m$ *with* $m \geqslant 1$ *and* $\mu_{\omega\chi^{-1}} = 0$, *then* $\lambda_\chi \leqslant (\lambda_{\omega\chi^{-1}}) - 1$.

Proof. Recall that M_∞^χ is the maximal abelian p-extension of K^χ which is unramified outside p. Let $\mathcal{M}_\infty^\chi$ be the maximal abelian p-extension of K_∞^χ which is ramified outside p and let $X_\infty(\chi) = G(\mathcal{M}_\infty^\chi / K_\infty^\chi)(\chi)$. If $G = G(M_\infty^\chi / K^\chi)$ and $X_0 = G(M_\infty^\chi / K_\infty^\chi)$, we have the following diagram.



Let $I(p) \subset X_\infty(\chi)$ be the inertia group for the unique prime in K_∞^χ which lies over p. If $X(\chi)$ is the χ-component of the Galois group of the maximal abelian unramified p-extension of K_∞^χ, then $X(\chi) \simeq X_\infty(\chi)/I(p)$. Since $\mu_{\omega\chi^{-1}} = 0$, Theorem 1 tells us that $X_\infty(\chi) \simeq \mathbb{Z}_p^{\lambda_{\omega\chi^{-1}}}$. We also know that $X(\chi) \simeq \mathbb{Z}_p^{\lambda_\chi} \oplus$ torsion. Thus, our theorem follows immediately if we can show that $I(p)$ is non-trivial.

Let $|A_0(\chi)| = p^r$. Then by taking the composite of the Hilbert class field of K^χ with K_∞^χ we know that M_∞^χ contains an unramified extension of K_∞^χ of degree at least p^r (in the χ-component).

Let $I \subset G$ be the inertia group for the unique prime of K^χ lying over p. Since G is abelian, $|G : I| = p^r$. We claim that the maximal unramified extension of K_∞^χ contained in M_∞^χ has degree exactly p^r. Since we have already established that its degree is at least p^r, we simply note that counting cosets tells us that $|X_0 : X_0 \cap I| \leqslant p^r$.

We now return our attention to $I(p)$. We want to rule out the possibility that $I(p) = 0$. This is easy, since the assumption that $m \geqslant 1$ forces some ramification to occur between K_∞^χ and M_∞^χ. Thus $X_\infty(\chi)$ contains ramification and $I(p) \neq 0$. This implies that $\lambda_\chi \leqslant (\lambda_{\omega\chi^{-1}}) - 1$. ∎

COROLLARY. *Under the hypotheses of Theorem* 3, *if* $|A_0(\omega\chi^{-1})| = p$, *then* $\lambda_\chi = 0$.

Proof. Theorem 2 says that $\mu_{\omega\chi^{-1}} = 0$ and $\lambda_{\omega\chi^{-1}} = 1$. Now apply Theorem 3. ∎

It is possible to put Theorem 3 and its corollary into a more general setting. Let L be a CM field with maximal real subfield L^+. Let λ, λ^+ be their respective λ-invariants corresponding to the cyclotomic $\mathbb{Z}_p$-extension of L. We set $\lambda^- = \lambda - \lambda^+$.

It is well known that if L contains a primitive pth root of unity then $\lambda^+ \leqslant \lambda^-$. Under certain hypotheses we can now say that we have strict inequality, i.e., $\lambda^+ \leqslant \lambda^- - 1$.

9. p-ADIC L-FUNCTIONS

We recall that k is a totally real number field, K is an abelian extension of k containing ζ_p, and $|\Delta| = |G(K/k)|$ is prime to p. Let $\chi \in \hat{\Delta}$ be a non-trivial even character. Deligne and Ribet have shown that there exists a p-adic L-function $L_p(s, \chi)$ associated to χ. They were able to show that there exists a $g(T, \omega\chi^{-1}) \in \Lambda$ with the property that $L_p(s, \chi) = g(\kappa_0^s - 1, \omega\chi^{-1})$.

As seen before, if X is the Galois group of the maximal abelian unramified extension of $K_\infty^{\omega\chi^{-1}}$ over $K_\infty^{\omega\chi^{-1}}$, then $X(\omega\chi^{-1}) \sim \Lambda/(f_{\omega\chi^{-1}}(T))$ where $f_{\omega\chi^{-1}}(T) \in \Lambda$. The main conjecture asserts that $f_{\omega\chi^{-1}}(T) = g(T, \omega_{\chi^{-1}})U(T)$ where $U(T)$ is a unit in Λ. Thus, the main conjecture says that an algebraic object (the characteristic power series $f_{\omega\chi^{-1}}(T)$) and an analytic object (the p-adic L-function $g(T, \omega\chi^{-1})$) differ by a unit.

If we assume that K^χ is an abelian extension of $\mathbb{Q}$, then Iwasawa's construction of the p-adic L-function shows that $g(T, \omega\chi^{-1})$ divides $f_{\omega\chi^{-1}}(T)$. We can then state the following.

PROPOSITION 2. *Under the hypotheses of Theorem 2, if K^χ is an abelian extension of $\mathbb{Q}$, then the main conjecture is true for k^χ. In fact, $L_p(s, \chi)$ has a unique zero α with $\alpha \equiv 1 \pmod{p^n}$.*

Proof. Since $A_n(\omega\chi^{-1})$ is non-trivial, it is clear that $g(T, \omega\chi^{-1})$ is not a unit. Since Theorem 2 says that $f_{\omega\chi^{-1}}(T) = T - a$ with $a \equiv p(\text{mod}\, p^n)$ and since $g(T, \omega\chi^{-1})$ divides $f_{\omega\chi^{-1}}(T)$, we see that $g(T, \omega\chi^{-1}) = f_{\omega\chi^{-1}}(T)U(T)$ with $U(T) \in \Lambda^\times$.

Thus, the main conjecture is true for K^χ.

Since $L_p(s, \chi) = g(\kappa_0^s - 1, \omega\chi^{-1})$ and since $g(T, \omega\chi^{-1}) = (T - a)U(T)$, we see that $L_p(s, \chi)$ has a unique zero. If we set $\alpha = \log_p(1 + a)/\log_p(\kappa_0) \in \mathbb{Z}_p$, then because $\kappa_0^\alpha - 1 = a$, we find that $L_p(\alpha, \chi) = 0$. Also, $L_p(s, \chi) = (\kappa_0^s - \kappa_0^\alpha)U(\kappa_0^s - 1)$ so that $L_p(1, \chi) = (\kappa_0 - \kappa_0^\alpha)U(\kappa_0 - 1)$. Since $\kappa_0^\alpha - 1 = a \equiv p(\text{mod}\, p^n)$ and since κ_0 may be chosen to be $1 + p$, we see that $\kappa_0 - \kappa_0^\alpha \equiv 0(\text{mod}\, p)$. Thus $\kappa_0 \equiv \kappa_0^\alpha(\text{mod}\, p)$, and it follows that $\alpha \equiv 1(\text{mod}\, p^n)$.

We note that Washington proved the above results for quadratic number fields using analytic techniques [Wa 2].

One may define an algebraic p-adic L-function to be equal to $f(\kappa_0^s - 1)$.

COROLLARY. *Under the hypotheses of Theorem 2, the algebraic p-adic L-function $f(\kappa_0^s - 1)$ has a unique zero α with $\alpha \equiv 1(\text{mod}\, p^n)$.*

10. QUADRATIC FIELDS

The previous theorems were motivated by theorems of Scholz [Sc] and Washington [Wa 2] concerning quadratic number fields. In this section, we specialize these theorems, and in particular we retrieve Washington's results. We also give several examples and show that the hypotheses of Theorem 2 are in some sense sharp.

Let $d > 0$ and assume that 3 does not divide d. We are interested in studying the following diagram:

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{-3}, \sqrt{d}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{-3d}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{-3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{d}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

The totally real field which we start out with in Theorem 2 is $k = \mathbb{Q}$ and the field K corresponds to $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$. Note that K contains a primitive cube root of unity, so the prime we are studying is $p = 3$.

Let $G(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ where

$$\begin{aligned}
\{1, \tau\} &= G(K/\mathbb{Q}(\sqrt{d})) \\
\{1, \sigma\} &= G(K/\mathbb{Q}(\sqrt{-3})) \\
\{1, \sigma\tau\} &= G(K/\mathbb{Q}(\sqrt{-3d})).
\end{aligned}$$

Let ω be the Teichmüller character, so that $\omega(\tau) = -1$ and $\omega(\sigma) = 1$. Let χ be the character defined by $\chi(\tau) = 1$ and $\chi(\sigma) = -1$. Then $K^{\omega\chi^{-1}} = K^{\omega\chi} = \mathbb{Q}(\sqrt{-3d})$ and $K^{\chi} = \mathbb{Q}(\sqrt{d})$. This was our motivation in previously studying $K^{\omega\chi^{-1}}$ and K^{χ}. Furthermore, if A is the 3-Sylow subgroup of the class group of K, then $A(\omega\chi)$ is the 3-Sylow subgroup of the class group of $\mathbb{Q}(\sqrt{-3d})$ while $A(\chi)$ is the 3-Sylow subgroup of the class group of $\mathbb{Q}(\sqrt{d})$. Thus, $A = A(\chi) \oplus A(\omega\chi) = A^+ \oplus A^-$.

In order to state Theorem 2 in this special case, we need to compute $F(\chi)$.

Since we are only concerned with the prime 3, we denote by $|b|$ the 3-adic absolute value of b. So, if $W(\mathbb{Q}(\sqrt{d}, \sqrt{-3}))$ is the multiplicative group of roots of unity in $\mathbb{Q}(\sqrt{d}, \sqrt{-3})$, then $|W(\mathbb{Q}(\sqrt{d}, \sqrt{-3}))| = 3$. Since $S_k = S_{\mathbb{Q}}$ only consists of the prime 3, $|1 - \chi(3)/N(3)| = \frac{1}{3}$.

Let ε be the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Then $R_3(\mathbb{Q}(\sqrt{d})) = \log_3(\varepsilon)$ where $\log_3$ denotes the 3-adic logarithm. Then in the notation of Section 7, $\mathcal{O}_p(\chi) = \mathbb{Z}_3 \sqrt{d}$ and $D(\chi) = \mathbb{Z}_3 \log(\varepsilon)$. So $(R_p(\mathbb{Q}(\sqrt{d}))/\sqrt{\operatorname{disc}(\mathbb{Q}(\sqrt{d}))})(\chi) = \log_3(\varepsilon)/\sqrt{\operatorname{disc}(\mathbb{Q}(\sqrt{d}))}$. Since we are only interested in the "3-part," we may just as easily consider $8 \log_3(\varepsilon) = \log_3(\varepsilon^8)$. The advantage of this is that by considering residue field degrees, we see that ε^8 is always congruent to $1 \pmod 3$.

Let 3^k be the highest power of 3 which divides $\varepsilon^8 - 1$, so that $\varepsilon^8 = 1 + 3^k(a + b\sqrt{d})$. Let $|A^+| = 3^m$. Then since $|\log_3(1+x)| = |x|$ and since 3 does not divide d, we have $F(\chi) = 3^{k+m-1}$.

Recall that we defined $e = \max\{n \mid K^{\chi}(\zeta_p) \supseteq \mathbb{Q}(\zeta_{p^n})\}$. Clearly $e = 1$ in this situation and since one prime ramifies in the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{-3d})$, we have the following.

THEOREM 2′. *Let $d > 0$ and assume that 3 does not divide d. Let ε be the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Let 3^s, 3^m, and 3^k be the highest powers of 3 which divide the class number of $\mathbb{Q}(\sqrt{-3d})$, the class number of $\mathbb{Q}(\sqrt{d})$, and $\varepsilon^8 - 1$, respectively. If $s = 1$ and $m + k \geqslant 3$ then the Iwasawa invariants μ_3^- and λ_3^- associated to the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{-3d})$ are 0 and 1, respectively.* ∎

We now specialize Theorem 3.

First, we must ensure that only one prime lies over 3 in $\mathbb{Q}(\sqrt{d})$. We do this by assuming that $d \equiv 2 (\bmod\ 3)$. Second, we must have $F(\chi)/|A^+| \geqslant 3$. Since $F(\chi)/|A^+| = 3^{k-1}$ we see that this assumption is equivalent to $k \geqslant 2$.

THEOREM 3′. *Assume that $d \equiv 2 (\bmod\ 3)$ and that $k \geqslant 2$. Let λ_3^+ be the Iwasawa invariant associated to $\mathbb{Q}(\sqrt{d})$. If A^- is cyclic and non-trivial, then $\lambda_3^+ \leqslant \lambda_3^- - 1$. If A^- is of order exactly 3, then $\lambda_3^+ = 0$.*

Proof. If $m = 0$, since one prime ramifies and it totally ramifies in the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{d})$, then it is well known that $\lambda_3^+ = 0$ (see, for example, [Wa 1, 13.22]).

If $m \geqslant 1$, then $m + k \geqslant 3$ and Theorem 3 says that $\lambda_3^+ \leqslant \lambda_3^- - 1$. If $|A^-|$ has order exactly 3, then $\lambda_3^- = 1$, so that $\lambda_3^+ = 0$. ∎

EXAMPLES. We now give several examples. The first is taken from [Gr 2] and the second from [Wa 2]. The final two examples show that Theorem 2′ is sharp in the sense that if $m + k < 3$, the value of λ^- is not necessarily one. Note that Theorem 3′ says that $\lambda^+ = 0$ in the first three cases but says nothing for the fourth:

d	s	m	k	λ	λ^+
257	1	1	3	1	0
97,865	1	3	1	1	0
62	1	0	2	2	0
82	1	0	2	1	?

ACKNOWLEDGMENT

I thank Larry Washington for his many helpful comments.

REFERENCES

[A.-F.] Y. AMICE AND J. FRESNEL, Fonctions zêta p-adiques des corps de nombres abéliens réels, *Acta Arith.* **20** (1972), 353–384.

[Co] J. COATES, p-Adic L-functions and Iwasawa's theory, *in* "Algebraic Number Fields" (A. Fröhlich, Ed.), pp. 269–353, Durham Symposium, 1975, Academic Press, New York/London, 1977.

[Fe] L. J. FEDERER, Noetherian $\mathbb{Z}_p[[T]]$-modules, adjoints, and Iwasawa theory, *Illinois J. Math.* **40** (1986), 636–652.

[Gr 1] R. GREENBERG, On the Iwasawa invariants of totally real number fields, *Amer. J. Math* **98** (1976), 263–284.

[Gr 2] R. GREENBERG, A note on K_2 and the theory of $\mathbb{Z}_p$-extensions, *Amer. J. Math.* **100** (1978), 1235–1245.

[Gr 3] R. GREENBERG, On p-adic L-functions and cyclotomic fields, II, *Nagoya Math. J.* **67** (1977), 139–158.

[Iw 1] K. IWASAWA, On $\mathbb{Z}_\ell$-extensions of algebraic number fields, *Ann. of Math.* **98** (1973), 246–326.

[Iw 2] K. IWASAWA, Lectures on p-adic L-functions, *in* "Annals of Math. Studies," Vol. 74, Princeton Univ. Press, Princeton, NJ, 1972.

[La] S. LANG, Cyclotomic fields, *in* "Graduate Texts in Mathematics," Springer-Verlag, New York, 1980.

[Sc] A. SCHOLZ, Über die Bezeihung der Klassenzahlen quadratischer Körper zueinander, *J. Reine Angew. Math.* **166** (1932), 201–203.

[Wa 1] L. WASHINGTON, Introduction to cyclotomic fields, *in* "Graduate Texts in Mathematics," Springer-Verlag, New York, 1982.

[Wa 2] L. WASHINGTON, Zeroes of p-adic L-functions, *in* "Sém. Delange-Pisot Poitou, Théorie des Nombres, 1980/1981," Birkhäuser, Boston/Basel/Stuttgart, 1982.